Regulating Complex Critical Infrastructure Risks: Evidence From the Electric Grid Cybersecurity Standards

Aaron Clark-Ginsberg
Associate Social Scientist, the RAND Corporation
Email: clarkginsberga@gmail.com | Twitter: @aclarkginsberg
ITI/CIRI Webinar Series, March 4th 2019
The 2003 Northeast Blackout

“...violations of existing [North American Electric Corporation] reliability standards contributed directly to the blackout.”

“...there are terrorists and other malicious actors who have the capability to conduct a malicious cyber attack with potential to disrupt the energy infrastructure.”
The electric grid depends on industrial control systems
The North American Electric Corporation (NERC) Critical Infrastructure Protection (CIP) Standards

• Mandatory, semi-prescriptive cybersecurity standards for the bulk electric system
• Developed by industry through NERC, with oversight from the Federal Energy Regulatory Commission
• Fines upwards of $1 million per day
• Evolving regulations
The NERC CIP Standards

002: Identify/categorize Bulk Electric System (BES)
  Cyber system risk level
003: Management (policies & planning)

004: Personnel & training

005: Electronic security perimeter

006: Physical security of cyber systems

007: System Security Management

008: Incident reporting & response

009: Recovery plans for BES systems

010: Configuration change management & vulnerability assessments

011: Information protection

014: Physical Security

High, medium, or low impact?
The NERC CIP Standards: Policy Questions

“NERC has taken a number of actions to protect the bulk power system against cyber security threats... We believe these efforts have improved and will continue to improve the reliability and security of the bulk power system.”
–Michael Assante, NERC’s Vice President and Chief Security Officer, speaking at a 2009 Congressional Hearing

“We have a culture of compliance when we should really have a culture of security.”
–Tim Roxey, NERC’s Director of Risk Assessment and Technology, 2011

“...the past three [presidential] administrations have consistently eschewed regulation as a policy solution for cybersecurity.”
(President’s Commission On Enhancing National Cybersecurity, 2016)

“[R]egulations are essentially being established by the entities who are being regulated. This may potentially be a conflict of interest.”
(Congressional Research Service, 2011)
The NERC CIP Standards: Broader Questions

“How tools of risk management and regulation help to prepare for recurring crises and disasters, such as hurricanes, earthquakes, technical break-downs and large-scale industrial accidents, critical infrastructure failures, epidemics, or invasive species, remains an important area for further scholarly attention.” (Boin and Lodge, 2016)

“There have been earthshaking changes in the relationship between the state, society, and private economic activity... Sociology cannot leave the discussion and analysis of regulation to stay in its error ridden, asocial, dangerous complacency.” (Perrow, 2015)
Research Question

How have the NERC CIP Standards shaped the way risks are managed in the electric grid?
Utility

- Provides one of the first sociological studies of how critical infrastructure cybersecurity standards function

- Offers a new way of understanding regulatory capture and expertise
Research Design and Methods

• Design: Qualitative and iterative approach focused on producing new knowledge and improving practice

• Data includes: semi-structured interviews with 70+ stakeholders, observational research at 20+ industry events, and documentary data

• Outputs include: conference presentations, government briefings, and articles
Findings

• Respondents described regulations as a dynamic and emergent regime involving interactions between many players. These interactions shape and are shaped by three related aspects of regulation:
  • **Incentives**: how regulations affect behavior
  • **Scope**: what regulations cover
  • **Adaptation**: how quickly regulations and regulated industries change

*These aspects emerge from the interactions between formal regulations and complex sociotechnical systems. They influence the effectiveness of the standards.*
The standards have not been sufficient to eliminate all vulnerabilities.

- System complexity means that “Murphy regularly finds its way into the utility business. Things like perfect storms happen all the time.”
- The standards are designed as minimalist regulations. They are a “start”, a “baseline”, and a “floor”.
- Standards include *Technical Feasibility Exceptions* for legacy industrial control systems that do not possess the functionality for strong IT security.

However, the regulations have had important positive effects...
The standards *increased* attention to security and resources for security.

“With NERC CIP, executives are going to make the decisions based on the impact to the entity. **Faced with the possibility of $1 million dollar a day per violation, eyes get opened, and you get a lot of attention**...So when I say that CIP has helped in that sense, it absolutely has. Just the utility that I came from, I think the **staffing level for the operations team that was supporting the control centers, it tripled with NERC CIP.**”

But much of this attention goes to compliance activities, rather than the basic security mission.
Some organizations were penalized for establishing policies that went **beyond** NERC CIP requirements and then failing to uphold them perfectly.

**Example:** NERC CIP requires organizations to review patches (security software updates) at least every 35 days, but some established more stringent policies:

“They put [every ten days] in their policy, and then one day someone takes fifteen days to review their patches... And **even though they’re still well within the 35 days they get penalized**...It happened enough that so many - lots of facilities are just gun shy...”
Some organizations ended up **reducing security and reliability to avoid compliance paperwork burdens.**

**Example:** Version 1 classified Black Start capabilities as “critical” and thus subject to regulations. As many as 25% of organizations chose to remove such capabilities rather than to maintain the compliance burden.
For some organizations with **good** security practices, NERC CIP **lowered** levels of security.
For some organizations with poor security practices, NERC CIP raised levels of security.
NERC CIP has a **leveling effect** across different organizations with different levels of security.

**Policy recommendation:** NERC and FERC should revise standards and auditing procedures to eliminate perverse incentives.
Key portions of critical infrastructure protection are **out of NERC CIP’s scope because of jurisdictional limitations.**

“...if you want to attack the U.S. now, I wouldn’t go after the bulk electric system, **I would go through the distribution system, because that’s currently unregulated.**” Distribution is “still mostly asleep at the wheel.”
Key portions of critical infrastructure protection are **out of NERC CIP’s scope because of jurisdictional limitations.**

“...the gas system isn’t NERC CIP compliant, and the supply chain isn’t NERC CIP compliant, and the transportation systems that carry coal on trains or on barges to the power plants... none of that is NERC jurisdictional either.”
Key portions of critical infrastructure protection are out of NERC CIP’s scope because of jurisdictional limitations.

“...it’s like the Maginot Line.”

**Policy recommendation:** DHS and PUCs should develop mechanisms to facilitate coordination between different infrastructure and regulatory sectors across jurisdictional levels to improve electric grid security.
The standards forced the creation of a **new industry** and the development of **organizational competency and expertise**.

- Standards created a stable set of customers, which helped to spur on an operational technology (OT) cybersecurity industry.
- OT cybersecurity expertise emerged *endogenously* with the standards.
- Conflict between different IT and OT experts fueled impressions of regulatory capture.
The standards were modified as needs changed but the process was slow. This hindered security and innovation.

“You look at CIP v1 right now and you compare it to CIP v5 – they’re not even the same universe. CIP v5 is so much better.”

“Technology changes at a much faster pace than the standards language”. As a result “[t]he laws lag behind the technology by years.”

**Policy recommendation:** To facilitate adaptation, NERC and FERC should work to establish standardized values and expertise related to cybersecurity.
Recap and Conclusions

• Regulations can help mitigate risk within complex systems, but create (positive and negative) emergent outcomes.

• Critical infrastructure protection regulations should be designed to match organizational dynamics and institutional configurations of the systems they are trying to protect.

• Further research on different types of regulations and on regulations in different infrastructure sectors is needed.
Additional resources
